CLAIMS

1. A network security apparatus for securing packet header information of a data packet, comprising:

a key exchanger adapted to derive a cipher key;

a translator adapted to translate predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key; and

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network.

2. A network security apparatus as set forth in Claim 1, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

3. A network security apparatus as set forth in Claim 1, wherein said translator is adapted to queue the data packet until said key exchanger has derived the cipher key.

4. A network security apparatus as set forth in Claim 1, wherein said key exchanger further comprises:

a timer adapted to reset at a predetermined time interval, wherein said key exchanger derives the cipher key when said timer resets and the data packet is present at said translator.

5. A network security apparatus as set forth in Claim 1, wherein the wide area network is the Internet.

6. A network security apparatus for securing packet header information of a data packet, comprising:

a random number generator adapted to generate a random number;

a translator adapted to translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network.

7. A network security apparatus as set forth in Claim 6, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host.

8. A network security apparatus as set forth in Claim 6, further comprising:

a timer adapted to reset at a predetermined time interval, wherein said random number generator derives the random number when said timer resets and the data packet is received by said translator.

9. A network security apparatus as set forth in Claim 6, wherein the wide area network is the Internet.

10. A network security system for securing packet header information of a data packet communicated between a first enclave and a second enclave through a wide area network, the system comprising:

a first communication device in communication with the first enclave and the wide area network, said first communication device adapted to receive the data packet, translate predetermined portions of said packet header information and place the data packet on the wide area network; and

a second communication device in communication with the second enclave and the wide area network, said second communication device adapted to receive and restore the

predetermined portions of the data packet and place the data packet onto the second enclave.

11. A network security system as set forth in Claim 10, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

12. A network security system as set forth in Claim 10, further comprising:

a key exchanger coupled to said first and second communication devices, adapted to derive a cipher key; and

a timer electrically coupled to said key exchanger, adapted to reset at a predetermined time interval.

13. A network security system as set forth in Claim 12,

wherein said key exchanger derives the cipher key when said timer resets and the first communication device receives the data packet, and

wherein said first and second communication devices translate the predetermined portions of packet header

information according to a cipher algorithm keyed by the cipher key.

14. A network security system as set forth in Claim 12, wherein said first and second communication devices are adapted to queue the data packet until the key exchanger has derived the cipher key.

15. A network security system as set forth in Claim 10, wherein the wide area network is the Internet.

16. A method for securing packet header information of a data packet, comprising:

deriving a cipher key;

translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key; and

communicating the data packet between a first enclave and a second enclave through a wide area network.

17. A method for securing packet header information as set forth in Claim 16, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

18. A method for securing packet header information as set forth in Claim 16 further comprising:

queuing the data packet until the cipher key has been derived.

19. A method for securing packet header information as set forth in Claim 16 further comprising:

deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said translating step.

20. A method for securing packet header information as set forth in Claim 16 wherein the wide area network is the Internet.

21. A method for securing packet header information of a data packet, comprising:

generating a random number;

translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

communicating the data packet between a first enclave and a second enclave through a wide area network.

22. A method for securing packet header information as set forth in Claim 21, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host.

23. A method for securing packet header information as set forth in Claim 21, further comprising:

deriving the random number at predetermined time interval if the data packet to be communicated has been presented to said translating step.

24. A method for securing packet header information as set forth in Claim 21, wherein the wide area network is the Internet.

25. A method for securing packet header information of a data packet, comprising:

receiving the data packet at a first communication device;

translating predetermined portions of packet header information;

sending the data packet to a second enclave through a wide area network;

receiving the data packet at a second communication device on the second enclave;

translating the predetermined portions of the data packet at the second communication device; and

placing the data packet onto the second enclave.

26. A method for securing packet header information as set forth in Claim 25, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

27. A method for securing packet header information as set forth in Claim 25, further comprising:

deriving a cipher key at a predetermined time interval if the data packet is presented to the first communication device; and

translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key.

28. A method for securing packet header information as set forth in Claim 27, further comprising:

queuing the data packet until the cipher key has been derived.

29. A method for securing packet header information as set forth in Claim 25, wherein the wide area network is the Internet.

30. A communication device adapted for processing packet header information of a data packet, the communication device being operable to:

derive a cipher key;

translate predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key; and

communicate the data packet between a first enclave and a second enclave through a wide area network.

31. A communication device as set forth in Claim 30, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

32. A communication device as set forth in Claim 30, the communication device being further operable to queue the data packet until the cipher key has been derived.

33. A communication device as set forth in Claim 30, the communication device being further operable to derive the cipher key at a predetermined time interval if the data packet to be communicated has been generated.

34. A communication device as set forth in Claim 30, wherein the wide area network is the Internet.

35. A communication device adapted for processing packet header information of a data packet, the communication device being operable to:

generate a random number;

translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

communicate the data packet between a first enclave and a second enclave through a wide area network.

36. A communication device as set forth in Claim 35, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host.

37. A communication device as set forth in Claim 35, the communication device further operable to derive the random number at predetermined time interval if the data packet to be communicated has been presented to the communication device.

38. A communication device as set forth in Claim 35, wherein the wide area network is the Internet.

39. A device for securing packet header information of a data packet, comprising:

means for deriving a cipher key;

means for translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key; and

means for communicating the data packet between a first enclave and a second enclave through a wide area network.

40. A device for securing packet header information as set forth in Claim 39, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

41. A device for securing packet header information as set forth in Claim 39, further comprising:

means for queuing the data packet until the cipher key has been derived.

42. A device for securing packet header information as set forth in Claim 39, further comprising:

means for deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said means for translating.

43. A device for securing packet header information as set forth in Claim 39, wherein the wide area network is the Internet.

44. A device for securing packet header information of a data packet, comprising:

means for generating a random number;

means for translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number; and

means for communicating the data packet between a first enclave and a second enclave through a wide area network.

45. A device for securing packet header information as set forth in Claim 44, wherein the predetermined portions of packet header further comprises:

identity information that identifies a sending host.

46. A device for securing packet header information as set forth in Claim 44, further comprising:

means for deriving the random number at predetermined time interval if the data packet to be communicated has been presented to the means for translating.

47. A device for securing packet header information as set forth in Claim 44, wherein the wide area network is the Internet.

48. A device for securing packet header information of a data packet, comprising:

means for receiving the data packet at a first communication device;

means for translating predetermined portions of packet header information;

means for sending the data packet to a second enclave through a wide area network;

means for receiving the data packet at a second communication device on the second enclave;

means for translating the predetermined portions of the data packet at the second communication device; and

means for placing the data packet onto the second enclave.

49. A device for securing packet header information as set forth in Claim 48, wherein the predetermined portions of packet header information further comprise:

identity information that identifies a sending host within the first enclave and a receiving host within the second enclave.

50. A device for securing packet header information as set forth in Claim 48, further comprising:

means for deriving a cipher key at a predetermined time interval if the data packet to be communicated has been presented to the first communication device; and

means for translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key.

51. A device for securing packet header information as set forth in Claim 50, further comprising:

means for queuing the data packet until the cipher key has been derived.

52. A device for securing packet header information as set forth in Claim 48, wherein the wide area network is the Internet.